Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Canceled).

2. (Currently Amended) The method ~~as claimed in claim 1~~ according to claim 11, wherein ~~said~~ the first operation ~~A(g,x)~~

a) is a Diffie-Hellman function ~~(G(gx))~~ $G(g^x)$, wherein G() ~~being~~ is an arbitrary, finite cyclic group G; or

b) ~~and said first operation~~ is an RSA function ~~xg~~ x^g.

3. (Currently Amended) The method ~~as claimed in claim 1~~ according to claim 11, wherein said first operation is ~~carried out~~ performed on a group G, wherein the group G is one of the following groups ~~selected from the group consisting of~~:

a) a multiplicative group F_q^* of a finite body F_q, in particular having

- a multiplicative group Z_p^* of the integers modulo of a prescribed prime number p;

- a multiplicative group F_t^* with t = ~~2m~~ 2^m over a finite body F_t of characteristic 2;

[•]

b) a group of units Z_n^* with n as a composite integer;

~~b)~~ c) a group of points on an elliptic curve over a finite body; ~~and~~ or

~~c)~~ d) a Jacobi variant of a hyperelliptic curve over a finite body.

4. (Currently Amended) The method ~~as claimed in claim 3~~ according to claim 13, wherein ~~said~~ the second key is a session key or an authorization associated with an application.

5. (Currently Amended) The method ~~as claimed in claim 1~~ according to claim 13, wherein the Diffie-Hellman method is used to ~~generate said~~ produce the second key.

6. (Currently Amended) The method ~~as claimed in claim 1~~ according to claim 11, wherein ~~said~~ the encoding is ~~carried out~~ performed with ~~said~~ the first key utilizing a one-way function, in particular a cryptographic one-way function.

7. (Currently Amended) The method ~~as claimed in claim 1~~ according to claim 11, wherein ~~said~~ data transmitted ~~data are~~ is confidential data.

8. (Canceled).

9. (Canceled).

10. (Canceled).

11. (New) An authenticating method, comprising the steps of:

a) performing a first operation by a first entity on a prescribed known value and on a value only known to the first entity to obtain an uncoded result of the first operation;

b) encoding the result of the first operation with a first key known to the first entity and to a second entity to obtain an encoded result of the first operation;

c) transferring a message from the first entity to the second entity, wherein the message comprises the encoded result of the first operation as well as the uncoded result of the first operation; and

d) decoding the encoded result of the first operation by the second entity with the first key and authenticating the first entity only using the message.

12. (New) The method according to claim 1, wherein the first operation is an asymmetric crypto process.

13. (New) The method according to claim 11, wherein the result of the first operation is a second key with which the first entity is authorized to undertake a service on the second entity.

14. (New) The method according to claim 13, wherein the second key is determined in relation to $G(g^{xy})$, by virture of the fact that the second entity performs a second operation $G(g^{y})$ with a secret number y known to only it, the result of this second operation is encoded with the first key and transmitted to the first entity in the form of a message.

15. (New) The method according to claim 14, wherein the message also comprises the result of this second operation, an identification or a time stamp in an uncoded form.

16. (New) The method according to claim 11, wherein the encoding is performed with the first key utilizing a symmetric encoding method.

17. (New) The method according to claim 11, wherein the message further comprises an identification of an entity or a time stamp in both an uncoded form and in an encoded form.

18. (New) An authenticating system, comprising:

a first entity and a second entity, the entities being provided with a processor unit, wherein,

a) said first entity being configured to perform a first operation on a prescribed known value and on a value known only to said first entity to obtain a result of the first operation;

b) said first entity being configured to encode the result of the first operation with a first key known to said first entity and to said second entity to obtain an encoded result of the first operation;

c) said first entity being configured to transfer a message from said first entity to said second entity, wherein said message contains the encoded result of the first operation and the uncoded result of the first operation; and

d) said second entity being configured to decode the encoded result of the first operation with the first key and said second entity additionally being configured to authenticate said first entity only using said message.